

< itc >

Blockchain Course ▪ December 2018 ▪ Syllabus

Introduction

- Evolution of Money
- Introduction to Blockchain

Cryptography

- Hash Functions
- Finite Fields and Elliptic Curves
- Elliptic Curve Cryptography
- Signing / Verifying Messages

Bitcoin

Basics

- Parsing Transactions
- Signing / Verifying Transactions
- Creating Transactions
- Script Parsing and Processing
- Address Construction / Private Key WIF Format Construction
- Network Message Parsing

Blocks and Mining

- Parsing Blocks
- Validating PoW
- Target and Difficulty Calculation
- Merkle Tree Construction
- Merkle Proofs
- SegWit

Wallets and Clients

- Bitcoin Core API
- HD Wallets (BIP 32/39/44)

Ethereum

Basics

- Smart Contracts
- Nodes
- Transactions
- Gas and Fees
- Ethereum Structure

Traditional and Decentralized Applications

- Decentralized Application Development
- Similarities and Differences
- Development Environment Setup
- Key Developer Tools

Smart Contracts

- Introductory Smart Contracts
- Inter-Contract Execution
- Inheritance
- Libraries and the Ethereum Package Manager
- Smart Contract System Design

Interaction with End Users

- Introduction to Web3
- Building Truffle for the Web
- Integrating with React
- Integrating with Metamask + Infura





Smart Contract Pitfalls, Testing and Debugging

- Dangers and Exploits
- Writing Tests
- Smart Contract Best Practices
- Formal Verification

Scaling Solutions

- Payment and State Channels
- The Lightning Network
- Developing a LApp
- Ethereum Plasma

Advanced Topics

- Privacy and Anonymity in Blockchains
- PoS / DPoS
- Proof of Space-time
- Hyperledger / Private Blockchains
- Summary - Technical Panel Q&A

